Who Should Get My Private Data in Which Case? Evidence in the Wild

Franziska Herbert
franziska.herbert@rub.de
Mobile Security
Ruhr University Bochum
Germany

Gina Maria Schmidbauer-Wolf
ginamariawolf@gmail.com
Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt
Germany

Christian Reuter
reuter@peasec.tu-darmstadt.de
Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt
Germany

ABSTRACT

As a result of the ongoing digitalization of our everyday lives, the amount of data produced by everyone is steadily increasing. This happens through personal decisions and items, such as the use of social media or smartphones, but also through more and more data acquisition in public spaces, such as e.g., Closed Circuit Television. Are people aware of the data they are sharing? What kind of data do people want to share with whom? Are people aware if they have Wi-Fi, GPS, or Bluetooth activated as potential data sharing functionalities on their phone? To answer these questions, we conducted a representative online survey as well as face-to-face interviews with users in Germany. We found that most users wanted to share private data on premise with most entities, indicating that willingness to share data depends on who has access to the data. Almost half of the participants would be more willing to share data with specific entities (state bodies & rescue forces) in the event that an acquaintance is endangered. For Wi-Fi and GPS the frequencies of self-reported and actual activation on the smartphone are almost equal, but 17% of participants were unaware of the Bluetooth status on their smartphone. Our research is therefore in line with other studies suggesting relatively low privacy awareness of users.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; • **Human-centered computing** → *User studies.*

KEYWORDS

data sharing, privacy, survey, awareness

ACM Reference Format:
Franziska Herbert, Gina Maria Schmidbauer-Wolf, and Christian Reuter. 2021. Who Should Get My Private Data in Which Case? Evidence in the Wild. In *Mensch und Computer 2021 (MuC '21), September 5–8, 2021, Ingolstadt, Germany.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3473856.3473879

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
MuC '21, September 5–8, 2021, Ingolstadt, Germany
© 2021 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-8645-6/21/09…$15.00
https://doi.org/10.1145/3473856.3473879

1 INTRODUCTION

Today 3.5 billion people in the world own a smartphone [28]. While using public space, people carry those smartphones and are in most cases probably not aware of the data that is produced and shared by that. Data emitted and produced through smartphone usage can be utilized in the users favor, e.g. by providing personalized support [20] and better services [24, 29]. In addition to this, sharing data can be beneficial in a variety of contexts such as personal health, calculating environmental impact, or forecasting weather [24, 37]. However, these benefits only arise if people share their data knowingly and voluntarily. Besides that, the security and privacy of the shared smartphone data is especially essential [20, 29] with regard to user acceptance. Therefore, users want to have information about when and with whom they share their data (e.g., [5]). The problem of the user's data being analyzed and used without the user's consent e.g. was acknowledged by Vincent et al. [48]. But to obtain this consent, users first have to be aware of the type and amount of data their smartphone produces and who can use that data. However, studies suggest that users are not very well informed about data privacy (e.g., [40], [5]). Smartphones contain many built-in sensors, such as GPS, proximity sensor, ambient light sensor, fingerprint sensor, and others. While some of them, like the fingerprint sensor for authentication, might be used intentionally, others might just be active without the users being aware of this. While some of these sensors offer convenient functionalitities for the user – with Bluetooth, for example, enabling contact tracing apps, as in the case of the Corona-Warn-App currently in use – privacy aspects also have to be considered [13]. Especially since the Covid-19 pandemic, Bluetooth has gained more attention in the public, as several contact tracing apps have been developed all over the world. In many countries, the development of these apps was accompanied by a debate about privacy and security aspects and the pros and cons of using Bluetooth for this purpose. Besides the useful application areas of Bluetooth, it can also pose a threat to mobile security as, for example, malware can spread from device to device. Moreover, GPS information can be used to gather information on movement profiles of users and to conduct information or even identity theft [25]. Using Wi-Fi can also have negative aspects like leading to transferred data being tapped [25]. In campaigns for mobile security, the German Federal Office for Information Security advises users to activate Bluetooth, Wi-Fi, and GPS only if necessary [17]. But do these campaigns bear fruits with regard to the overall awareness in the German population? Do people know which of these functionalities are activated and do they activate or deactivate them on purpose? Which kind of data do Germans

view as private and with whom and under which circumstances would they like to share it? To gain insight into these questions, we conducted a representative online survey with 1,030 German participants as well as 58 brief face-to-face interviews in the streets of the German city Darmstadt, which has roughly 150 thousand inhabitants.

This paper aims to contribute to research on users' perception of sharing personal data. In order to answer the research question **"When and why do people (in Germany) share private data through smartphones voluntarily, conditionally, or involuntarily?"** we want to address the following sub-questions:

(1) RQ1: Which kind of data is perceived as private data? (online survey)
(2) RQ2: When and with whom are people willing to share their private data? (online survey)
(3) RQ3: When and why are functionalities such as Wi-Fi, Bluetooth, and GPS activated and are people aware of that? (online survey & street interviews)

In the following sections, related work (section 2) and the applied methods (section 3) are presented. After the illustration of the results of the online survey (section 4.1) and the street interviews (section 4.2), the findings are discussed in a broader context (section 5) and conclusions are drawn (section 6).

2 RELATED WORK

In this section we cover related work concerning the overall circumstances of conscious and voluntary data sharing as well as the threats that can arise from that. We also report on users' privacy literacy and data sharing behavior. Ethical considerations regarding private data sharing in public spaces and the use of that data are additional relevant aspects, but beyond the scope of this paper. Instead, we focus on investigating users' awareness and habits of sharing private data.

2.1 Use Cases of Voluntarily Providing Smartphone Data

In this section we provide related work on use cases of voluntarily providing smartphone data by first outlining benefits and potentials of data sharing and subsequently describing negative aspects and threats.

2.1.1 Benefits and Potentials. Use cases for smartphone data are diverse with many of them bringing forward improvements for users by sharing data knowingly and voluntarily, often via specific apps. In this context, Rehman et al. [20] conclude that Big Data personalization may offer benefits such as better patient, traveler, or customer experience, but needs to be privacy preserving. Lau et al. [29] propose using the data voluntarily contributed by public transport passengers' smartphones for getting real-time public transport data. In this way, the data generated and provided by users can be useful for other users of the same infrastructure. They identify trust and privacy as key acceptance factors for data sharing. Niforatos et al. [37] developed and presented an application which utilizes smartphone sensors as well as users' input regarding current and estimated future weather, to forecast weather. They find that for this use case, combining sensor data with user input is more accurate than using only the sensors. Another use case for providing self-generated data is gaining money in exchange for data [35]. Collecting data with the voluntary consent of users can also help to improve the urban quality of life, especially regarding public safety. Although well-recorded incident data suggests a specific area to have a high level of public safety, they could still be perceived by citizens as unsafe [44]. Therefore, Garzon and Bersant [44] suggest that citizens should report it if they feel unsafe via a mobile app by using users' location data. Ranchordás [41] looks at how Internet of Things (IoT), Big Data, and algorithms can be used to nudge citizens towards a certain, desired behavior such as saving resources, using public transportation, or increasing participation in local affairs. Systematic nudging might lead to smart cities achieving their sustainability goals; therefore, it can be considered well intended in these cases. In contrast, there are ethical and legal issues related to the collecting and processing of large amounts of personal as well as impersonal data in order to influence citizens' behavior. Masdeval et al. [31] propose the usage of citizens reporting their concerns digitally and the analysis of citizens' emotions in order to estimate the urgency of urban issues. While users consciously and deliberately provide the issues, the urgency shall be estimated through text mining looking for emotions in the user generated free texts [31]. The current Covid-19 pandemic also shows that using sensor data from smartphones can help to contain the spread of the virus. Widespread downloads of the German Corona-Warn-App (24.9 Mio., as of January 2021) [43] show that users value its impact and make trade-offs in terms of data sharing and personal benefits.The privacy for benefit trade-off (e.g., private data for services or money) has been found in a variety of contexts, such as social network sites, e-commerce and mobile application [7].

2.1.2 Negative Aspects and Threats. Besides the described useful applications of data sharing, possible negative effects and potential barriers, especially with regard to privacy and security have been covered in the literature. Cao et al. [12] argue that data sharing can only maximize its potential if a multitude of people share their data. In order to encourage that, trust is needed because its absence could negatively affect the willingness to share personal data. As transparency and accountability are key factors for the acceptance, Cao et al. [12] propose a trust model for data sharing in smart cities. In this context, Kalimaris and Pitsillides [23] summarize research on the connection of mobile phone data with IoT/Web of Things (WoT) and highlight - beside many benefits - challenges and open issues such as privacy protection and security. Data insecurity is a threat for users' data. In a study by Balebako et al. [5] on data leaks in mobile games, such as 'Angry Birds', 14 out of 19 participants saw no benefit at all with regard to data sharing. Within the study, the authors asked participants about what they thought, what kind of data is shared by playing games on their smartphones. The responses of the participants could be categorized in three groups, one believing no data left the smartphone, one thinking the data was only shared with the app developers and one believing that data was also shared for marketing purposes [5]. After showing participants, via a prototype tool, what kind of data was shared during their short time of playing the game, participants across all groups were surprised about how frequent data was shared and

with which entities. Felt and colleagues [16] found that concerns on data sharing depend on who the data is shared with. They asked participants to rate their feelings about the risks of allowing apps to access smartphone sources ("indifferent" to "very upset"). For sharing location data publicly almost 71.57% indicated they would be feeling very upset, while less participants would feel very upset when sharing their location with advertisers (62.8%), or with friends (58.10%). They also found women feeling significantly more upset about potential data sharing than men.

2.2 Usability and Privacy Literacy as Influencing Factors on Data Sharing

In general, data sharing is influenced by many factors, such as privacy requirements and trust as described above. Further important influencing factors also include usability and privacy literacy, as previous research has shown. A user study by Watson and Zheng [49] found that mobile phone users do not follow security recommendations but rather favor usability over security. Favoring usability or utility (e.g., services offered, cost of use, user base) is a phenomenon that is also known from other contexts of usable security, as for example encrypted e-mail and messaging (e.g., [1], [51]). To limit exposure, users are generally advised to turn off Wi-Fi, Bluetooth, and GPS when not needed. However, most participants left their Wi-Fi on by default and almost half of the participants proceeded the same way with GPS on their phones. For Bluetooth on the other hand, the majority of participants did not leave it on by default. The authors conclude that users need to be made aware of mobile threats and mobile security [49]. Similarly, Ali et al. [3] found more than half of over 3,000 smartphone users not to be aware of smartphone security and privacy. While [10] found that security behavior significantly differs between age and education groups (younger and less educated show less security behavior), no such differences could be found for privacy behavior. Park and Jang [40] also report low privacy literacy for young African Americans, with most participants only sparsely being aware about the risks of information-location surveillance and not being able to perform simple privacy setting changes. Bartsch and Dienlin [8] found that online privacy literacy is a mediator for behaving secure and privacy conform and conclude that having more experience with the Internet leads to more online privacy literacy. Park et al. [39], similarly, found privacy knowledge (e.g., knowledge of data collection risks) to be a significant predictor of higher levels of privacy protection.

2.3 When and With Whom Do Users Want to Share their Data?

Helen Nissenbaum's [38] theory of privacy as contextual integrity states that the appropriateness of the personal information flow depends on informational norms, with key parameters of these norms being actors (e.g., recipient), attributes (e.g., data types), and transmission principles (e.g., constraints for data transmission such as confidentiality). These parameters are important in order to examine when users are willing to share their data under which conditions and in which context. Nicholas et al. [36] asked users on their comfort of sharing sensed health data (physical activity, sleep, mood) and personal data (location (GPS), communication logs, social activities) with different receivers (doctors, electronic health record (EHR), and family members). They found that users were more comfortable with sharing health data than with personal information. Additionally, users were also more willing to share either data with doctors than with EHR or family and least comfortable with sharing their location with any of the receivers. Based on these results, we included both data recipient and sharing context as relevant aspects in our questions concerning the willingness to share private data. Another study asked participants who they would share their location bases data with and found that almost half the participants did not see the need to specify with whom they would share that data. 49% of the participants chose public sharing while 3% chose no sharing [11]. Additionally, they asked participants for what services (that required that data) they would trade their long-term location trace data to a company for. Many participants indicated to trade this data for many services, such as personal traffic, home heating, bus route planning and traffic jams [11].

Nakagawa et al. [35] propose a framework that enables users to pick and sell their private data. They conducted a questionnaire with 131 people, asking about the cases in which users were willing to share their data with companies. They provided different private data topics (e.g., food costs, medical expenses, or taxes) and three cases of identification (1-no identification possible, 2-few identifications possible, 3-several identifications possible). They found that people provided data more willingly when no or few identifications were possible. Furthermore, private data was more freely shared when the data was about consume good expenses or food data as opposed to more personal data such as medical expenses or taxes. In an open question they asked what people wanted as an incentive to share their data and postulate that the answers are too various to draw conclusions. In their literature review, Gao et al. [19] found that incentives are a key factor for data sharing as they not only enable initial data sharing but also ensure this in the long-term. Incentives, such as money, competition, and comparison can improve the accuracy, coverage, and timeliness of sensor data sharing. Hann et al. [21] found that users are willing to put aside their privacy concerns for economic benefits (money). Arakawa and Matsuda [4] researched the impact of gamification to help (long-term) participatory sensing and found that gamification can have a positive influence and therefore consider it as a promising technique for getting users to provide their smartphone data. Lau et al. [29] identify trust and privacy as key acceptance factors for data sharing. Kleek et al. [26] conclude that transparency about tracking behavior is important, as some users otherwise limit the use of application.

2.4 Contribution to the Research Community

As stated in the sections before, prior research enables insights into the questions of how beneficial data sharing can be, how privacy aware users are with their online data, what threats arise from data sharing as well as which incentives it takes for users to share their data. However, taking into account the steadily increasing number of people owning smartphones, the emergence of new applications and ideas for using shared user data, and the focus of many studies on users in the USA, it is worth taking the topic of data sharing

behavior under investigation within Germany since generally, privacy attitudes and behavior can differ between cultures [30]. By means of a mixed-method approach of a comprehensive and representative online survey along with a smaller sample of face-to-face interviews, our research contributes to the understanding of smartphone users' data sharing behavior, by providing insights into a representative sample of German users as well as into evidence of actual behavior, respective smartphone settings, in Germany. We investigate which kind of data people view as private and with whom they would share it under different conditions. We contribute to prior research by assessing explicitly when and why users turn on or off Wi-Fi, Bluetooth, and GPS. Moreover, we are able to compare self-reported answers with actual behavior by inspecting the users' smartphone settings with them in 58 face-to-face street interviews. This represents a crucial point, as statements about one's own behavior can differ substantially from the actual behavior. For the development of our survey and interviews, we took Nissenbaum's [38] theory of contextual integrity into account. With current developments mind, such as smart city applications and apps using user data to benefit users, it is important to assess users' sharing behavior and habits of using Wi-Fi, Bluetooth, and GPS, which not only enable data sharing but may also be gateways for privacy and security threats.

3 METHOD

To gain insights into the question of which data people are willing to share under which conditions and why, when they switch functionalities such as Wi-Fi, Bluetooth, and GSP on and off, as well as to compare these preferences to their actual behavior, we conducted an online survey. Additionally, we conducted short personal face-to-face street interviews, since a survey can only assess self-disclosure and there is no possibility to verify the participants' responses. By collecting data from the participants' smartphones and putting them into context with the respective self-reports, as we did in the interviews, we follow the recommendations of Harari et. al [22]. The data obtained in this way was analyzed using Microsoft Excel, R 3.6.2, and RStudio. The open answers gained from the short interviews as well as from the online survey were analyzed using open coding. In the following sections, we introduce our survey method, the interview design, as well as our analysis plan and provide a sample overview.

3.1 Online Survey

To answer the three research questions (Which kind of data is perceived as private data? When and with whom are people willing to share their private data? When and why are functionalities such as Wi-Fi, Bluetooth, and GPS activated and are people aware of that?), we conducted a study representative for the German population over 18 years old in November 2019, using the online survey tool LimeSurvey and the certified online panel provider respondi. The sample (N = 1,030) was adapted to the distribution of age, region, and education according to the general German population [18]. Participants were recruited in Germany based on the mentioned criteria, wherefore our sample consisted of Germans exclusively. Due to occasional false answers to our quality check question, we had to eliminate the answers of some participants for our analysis. For this reason, our sub sample shows slight differences to the representative sample.

The online survey consisted of 46 questions in total, from which 13 questions were directly related to the research questions. First, the participants were asked which smartphone with which operation system they are using, at what times of the day their smartphone is switched on and which of the functionalities including Wi-Fi, Bluetooth, and GPS, they (think they) use and when they use them. Afterwards, the participants were asked about which of their data they perceive as private and who they want to know and share these data with. To enhance the answer quality, we implemented the following quality check question within question QO12: "Check the second left column". For the development of our questionnaire, we used the applicable guidelines for item design: Items should be phrased positively, clearly, short, concisely, and understandably. In addition to technical terms and universal expressions, like never and ever, assessments and leading questions should be avoided [33]. For gathering demographic information, we asked participants to indicate their identified gender, with the options "female", "male", "other" and "I don't want to answer this question". We did also asked participants to state their age, the state of Germany they live in and their education level. The questions were posed in German to avoid distortions due to misunderstanding. Before rolling out the questionnaire to the panel, we conducted a small pretest with 5 participants to investigate whether all questions are understandable. As the pretest revealed no problems with item comprehensibility, we rolled out the questions that can be found with an English translation in Appendix A.1.

3.2 Interview Design

The online survey assessed self-disclosure, as typical for online surveys. Additionally, we sought to compare this self-disclosure of technology use to actual technology use and therefore conducted face-to-face interviews in the streets of a German town. The short interviews were conducted by four researchers in November and December of 2019. Passers-by were asked to voluntarily participate and there were no specific criteria which upon they were selected. Participants were not compensated for their participation. Prior to the interview, participants were informed about the topic and time span and had the opportunity to withdraw. The interview took around ten minutes and the participants' answers were noted by the interviewers. In total 58 people participated in the interviews. The interviews consisted of eight closed questions, with two questions additionally consisting of open follow up questions, asking participants to state reasons for their answers (QS5, QS6). Participants were, among other things, asked if they owned a smartphone (QS1), at which times it is typically switched on (QS2), which operating system they use and which functionalities (Wi-Fi, Bluetooth, GPS) they have switched on/off and when (QS5). After asking participants about their current Wi-Fi, Bluetooth, and GPS status (switched on or switched off) we verified their answers by looking on their current smartphone settings (QS7, QS8). As well as in the online survey, we wanted to get some demographic information and asked participants to state the gender they identified with and their age. To disclose this information, as all other information as well, was optional for the participants and we did ask these as open

Table 1: Demographic Information of online and interview sample.

		Online survey sample (N = 980)		Interview sample (N = 58)	
		n	rounded %	n	rounded %
Gender	Female	508	52%	28	48%
	Male	472	48%	30	52%
Education	Currently student	17	2%	1	2%
	No degree	5	1%	2	3%
	Basic school degree (German Hauptschulabschluss)	292	30%	3	5%
	Secondary school degree (German Realschulabschluss)	320	33%	7	12%
	High school degree (German Abitur & Fachabitur)	192	20%	20	34%
	University degree	154	15%	25	43%
Smartphone possession	Yes	914	93%	58	100%
	No	63	6%	/	/
	I do not know	3	<1%	/	/
Operating system	Android	714	78%	32	55%
	iOS	178	19%	26	45%
	Other	7	1%	/	/
	I do not know	15	2%	/	/
		M	Min - Max	M	Min - Max
Age		47	18 - 74	32	14 - 75

questions with no provided response alternatives. All questions were also posed in German to avoid distortions due to misunderstanding. The questions and corresponding English translations can be found in Appendix A.2.

3.3 Analysis and Sample

The closed questions of both survey and interviews were analyzed descriptively using Microsoft Excel, R 3.6.2, and RStudio. First, we evaluated the quality check question, as we did not consider answers to closed questions of participants failing the quality check question. We did, however, include their open answers in the analysis if they answered those. The results of the open questions were analyzed via open coding by two researchers jointly. We first assigned codes to the text and analyzed the code frequency afterwards. This mixed-method approach is suggested by Mayring [32]. For the online survey, we also used chi²-tests to investigate the relation of perceiving data as private and the identified gender as well as the installed operating system.

After analyzing the quality check question and eliminating participants with wrong answers, the online survey sample used for further data analysis consisted of 980 participants. Of these, 508 participants identified their gender to be female and 472 identified as male. None of the participants identified as non-binary. Participants' age ranged from 18 to 74 years (M=47 years) and most participants owned a smartphone (n=914) with Android as the operating system (n=714). Participants taking part in the street interviews were between 14 and 75 years old, 30 participants identified their gender to be male and 28 participants identified as female. Again no participant identified as non-binary. Most of the participants were between 20 and 29 years old (33 out of 58 participants), whereas only one person was older than 70. This might be due to the topic of the interview, as some elderly people were initially interested to participate but withdrew after they heard what the interview was about. Table 1 provides information on the collected demographic information of the two samples.

4 RESULTS

In this section, we provide the results of the online survey as well as the results of the street interviews. We analyze the results in the order of the research questions, starting with RQ1: Which kind of data is perceived as private data? followed by RQ2: When and with whom are people willing to share their private data? RQ3: When and why are functionalities such as Wi-Fi, Bluetooth and, GPS activated and are people aware of that? We present the results of the online survey first, followed by the results of the interviews.

4.1 Online Survey

Out of the 980 participants, 914 possess a smartphone, 63 do not possess a smartphone, and three participants are unsure if they possess a smartphone. Thus, the results on smartphone use are based on the answers of 914 participants. For all questions concerning only privacy attitudes, we consider the answers of all 980 participants.

4.1.1 Which kind of data is perceived as private data? Figure 1 shows the results for research question one. Overall, most participants view all the data types as private. Since no more than one person did not respond to this question, this shows that nearly all participants have an opinion about what they consider private. Bank account details are perceived as private by the most participants, followed by the identity card number, personal files (such as photos and documents), personal communication (such as calls),

personal address, date of birth, and name. Chi²-tests reveal significant systematic relations between the gender and the perception of data as private for the following data types: address (chi^2=12.23, $p<0.05$), personal files (chi^2=7.34, $p<0.05$), bank details (chi^2=6.50, $p<0.05$), name (chi^2=4.83, $p<0.05$), and personal communication (chi^2=4.71, $p<0.05$). Significant and higher chi^2 values indicate a significant and greater relation of the two variables gender and data type. For all these types of data, more female users classify them as private than male users do. For details see Table 2. No significant systematic relations are found for the installed operating system and perceiving data types as private.

Table 2: Chi²-test perceiving data as private, gender differences – online survey.

Data type	Gender	Perceived as private (n)	Not perceived as private (n)	Chi²	*p*
Address	Female	435	73	12.23	<0.05
	Male	362	110		
Personal files	Female	454	54	7.34	<0.05
	Male	392	79		
Bank details	Female	499	9	6.50	<0.05
	Male	449	23		
Name	Female	325	183	4.83	<0.05
	Male	268	203		
Personal	Female	439	69	4.71	<0.05
communication	Male	382	89		

4.1.2 When and with whom are people willing to share their private data? Figure 2 shows the percentages at which participants would share private data with different entities. There are differences with whom people want to share data for different sharing options. Among all entities the option with *explicit allowance per situation* is among the most chosen options with 21% (entity: rescue services) up to 46% (entity: chosen services such as Google) of participants choosing it. This shows that people want to control who they share their private data with and would actively and voluntarily share their private data. The sharing option *never* is also one of the frequently selected options by participants, ranging from 16% (entity: chosen people) to 31% (entity: chosen services such as google). Between 8% (entity: chosen services such as Google) and 24% (entity: chosen people) of participants would share their private data *always* with different entities. The sharing option *If I am endangered* is most popular with the entities rescue forces (26%) and state bodies (13%, 9%). *If human lives can be saved* 16% of the participants would share their private data with rescue forces and 11% of participants would share their personal information with state bodies such as the police. *If potential harm for other people could be reduced* 14% of the participants would share their private data with state bodies such as the police and 9% would share their data with state bodies such as governments and rescue forces.

We asked participants if they would be more willing to share private data if a personally known person was endangered (see Table 3). Almost half of the participants (48%) answered that question with 'yes' or 'rather yes', for 37% of participants this would not make a difference, and the remaining 15% answered with 'no',

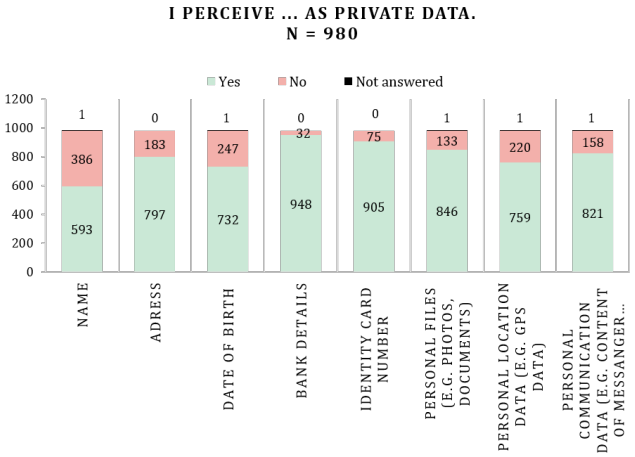

Figure 1: Data perceived as private – online survey.

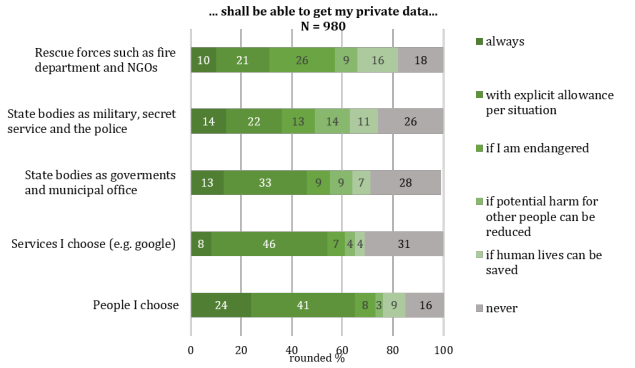

Figure 2: Answers to "Who shall be able to view my private data in which cases?" – online survey.

'rather no', or 'I do not know'. This shows that helping endangered acquaintances would increase data sharing willingness (with state bodies or rescue forces) for almost half of the participants.

Table 3: Answers to "I would possibly be more willing to share my private data with state bodies or rescue forces if I personally knew an endangered person." – online survey.

I would possibly be more willing to share my private data with state bodies or rescue forces if I personally knew an endangered person.					
Yes	Rather yes	Does not make a difference	Rather no	No	I do not know
19%	29%	37%	2%	8%	5%

4.1.3 When and why are functionalities such as Wi-Fi, Bluetooth, and GPS activated? Figure 3 gives insights into research question three. Around three to seven percent of the participants do not know what Wi-Fi, location services (GPS), and Bluetooth are or do not care whether they activate these or not. The percentage values for the option "I do not know" are around 1% for all functionalities. Most

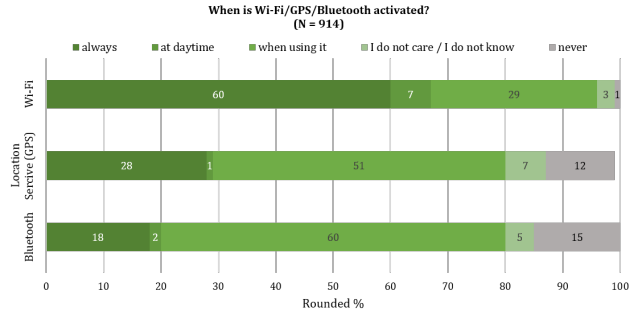

Figure 3: Answers to the questions "When is Wi-Fi, GPS, and Bluetooth activated on your smartphone?" – online survey.

participants (67%) have their Wi-Fi switched on either at daytime or always. 29% of participants switch on their Wi-Fi when needed and only 1% never switches it on. For both location services (GPS) and Bluetooth, most participants (51% and 60%) activate these when using them, compared to 29% and 20% having these functionalities activated at their smartphone always or at daytime. 12% and 15% of participants indicated to never switch on their location services (GPS) and Bluetooth on their smartphone.

Table 4: Reasons for switching location services (GPS), Wi-Fi, and Bluetooth off – online survey.

Why do you activate or deactivate location services (GPS), Wi-Fi, or Bluetooth?		
Category	Examples	Quantity named (N = 836)
Usage need	"to use home Wi-Fi" "location services for Google Maps" "because I need to use it"	417
No need to use	"I never use Bluetooth" "I do not need Bluetooth" "If I do not need it, I switch it off"	85
Privacy reasons	"due to privacy" "make tracking more difficult" "I do not want these apps to know my location and produce movement patterns"	70
Security reasons	"I deactivate location services and Bluetooth to feel save and so nobody can access my location easily" "If location services are switched on, I feel monitored and I think my data will be passed on" "Because of the threat of fraud"	79
Laziness	"laziness" "to use apps and other services comfortably" "it is more comfortable than switching it on and off all the time"	53
Economic reasons	"Wi-Fi is always on to save data capacity" "only when I use it, this saves battery capacity" "GPS and Bluetooth need to much battery capacity"	176
I do not know	"I do not know"	27
Other reasons	"to reduce radiation" "I switch off Bluetooth as I learned that it might lead to impotence" "I switch my smartphone off at night"	33

Table 4 shows the reasons for switching Wi-Fi, location services (GPS), and Bluetooth on or off, with most participants activating the functionality when needed. Participants switch them off due to economic reasons such as high battery and energy consumption (n=176), but also due to privacy (n=70) and security reasons (n=79). People fear tracking for example as a privacy threat and fraud as a security threat. 53 participants stated not to switch the services on or off for reasons of laziness: "it is more comfortable than switching it on and off all the time".

4.2 Street Interviews – When and why are functionalities such as Wi-Fi, Bluetooth, and GPS activated and are people aware of that?

Figure 4 provides additional insights into research question three. Evaluating the street interviews, one to seven percent of participants do not know what Wi-Fi, Bluetooth, and GPS are or do not care whether they have them activated or not. The exact percentages for the option "I do not know" are zero for Wi-Fi, 4% for location services and 3% for Bluetooth. Similar to the online survey most participants (69%) have their Wi-Fi either switched on at daytime or always. 24% of participants activate their Wi-Fi when needed and only 5% never switch it on. For both location services (GPS) and Bluetooth, many participants (47% and 47%) use the function when needed, compared to 23% and 19% having it activated on their smartphone always or at daytime. These frequencies are somewhat similar to the ones represented in the online survey. 25% and 26% of street interview participants indicated to never switch on their location services (GPS) and Bluetooth at their smartphone, these percentages are higher than in the online survey (12% and 15%).

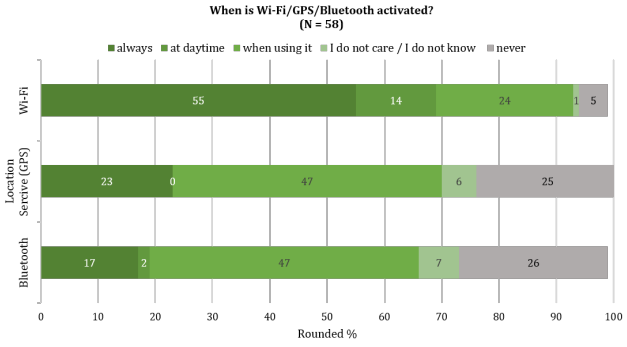

Figure 4: Answers to the questions "When are Wi-Fi, GPS, and Bluetooth activated on your smartphone?" – street interview.

In the street interviews, the aim was also to assess whether the self-reported activation status of Wi-Fi, GPS, and Bluetooth matches the actual activation status. The interviewers therefore asked participants to show them their smartphone settings. Table 5 shows frequencies for interview participants reported status of Wi-Fi, location services (GPS), and Bluetooth and the actual status (switched on vs. switched off). With regard to Wi-Fi and GPS, the actual status only slightly differed from what participants reported. The most striking differences between actual and reported status can be observed for Bluetooth. The actual status was different in

17% of the cases compared to the self-reported status. According to self-reported responses, GPS and Bluetooth were less frequently turned on than the actual status revealed. This shows that even though participants thought they would know the status of their smartphones' Wi-Fi, location services (GPS), or Bluetooth, not all are aware of the actual status.

Table 6 shows the reasons for switching Wi-Fi, location services, and Bluetooth on or off, with most participants activating the functionalities when they actually need them. Similar categories as in the online survey emerged also for the street interviews. Participants in the street interviews indicated to switch off the services also due to economic reasons such as high battery and energy consumption (n=9) and due to privacy reasons (n=16). In contrast to the online survey, no security reasons were mentioned. Most participants (n=32) activate the functionalities when they actually use them, e.g., active GPS to use Google Maps. 11 participants mentioned other reasons such as "mood" for switching services on or off. All answers in the category "Other reasons" were only named once.

5 DISCUSSION

Our study shed light on users willingess to share private data with different entities and their reasons for that. In this section we discuss the results of our study and point out its limitations.

5.1 Limitations

Although we carefully chose the questions contained in our sample and used pilot testing as well as a panel provider to increase data quality, our study has the following limitations. One limitation is the small and therefore not representative amount of actual functionality activation information derived from the street interviews. Additionally, our sample only consisted of women and men, not representing people with non-binary gender. It has to be noted that our sample consisted only of Germany and can therefore not be generalized for other countries. Importantly, our data collection took place prior to the Covid-19 pandemic, which might have changed perceptions and behaviors of data sharing. This should be examined in future studies. Generally, with regard to the online survey data it needs to be considered that self-reports do not necessarily represent a fully accurate description of actual behavior and settings. With our approach we shed light on this phenomenon and show, for example, that presumed smartphone settings sometimes differ from actual smartphone settings.

5.2 Factors Related to the Perception of Private Data

All the data types we studied, were viewed as private by the majority of participants, with bank details being rated as private by almost all participants. We assumed a relation between rating data types as private and the factors installed operating system and gender but could only find significant relationships for the latter. Our results show, that for almost all types of data significantly more female participants classified data types as private than male participants did. This is in line with other studies that found women to have higher privacy concerns than men [6, 16, 34, 45]. Another factor that might contribute to the high ratings of data types as private might be the socio-cultural characteristics. Other studies have found difference between countries with regard to social media use during emergencies [42], to privacy concerns [9], to trust social network sites [27], and to the willingness to adopt apps against the Covid-19 Pandemic [47]. German participants showed only low social media use compared to other European countries [42] and showed less trust in social media sites compared to participants in the US [27]. Concerning corona apps [47] found German participants to have lower acceptance for such apps than Chinese participants but higher acceptance than participants from the US. This study did also find high privacy values for German participants. We picked Germany and Darmstadt in particular for this study, because our university is located there and the conduction of face-to-face interviews there was the most economical way. The present study might have different outcomes in other countries.

5.3 The Role of Data Type and Data Receiver

Our results show that users' willingness to share private data is linked to the data type and the data receiver. Users queried in this study generally want to share their data, but with different quotas for certain circumstances and recipients. Especially when the receiving entities are services or acquaintances, many people (46%, 41%) want to decide depending on the situation whether they share their private data with these entities. However, except for services chosen by the users, more than 10% of users would always share their private data with the other entities. We suppose, users do that for convenience reasons, similar to why they have Wi-Fi, GPS, and Bluetooth always activated. On the other hand, concerning all entities (rescue forces, state bodies, self-chosen services, self-chosen people) more than 16% of people would never be willing to share their private data regardless of the recipient. The highest non-sharing-attitude was found for services such as Google. We can only assume, that this might be due to missing incentives or a lack of transparency and trust in these services. Users would rather share their data when they themselves are at risk than when other people are endangered. This is also highlighted by the fact that 39% would not be more (or less) willing to share their private data if an acquaintance was endangered. However, almost half of the participants would share more data with state bodies or rescue forces in this specific case. These findings underline the importance of transparency in terms of the recipient and the purpose of the transmitted data and the importance of control over the own data, as also proposed by previous research (e.g., [26]). The relevance of control over the own data was also found when researching contact tracing apps against the spread of SARS-CoV-2 [47].

Sharing private data at all times without incentives, which has also been proposed by literature (e.g., [19], [21]), does not seem to be attractive for most users. According to our study results, 16% up to 31% of users never want to share their private data with entities such as services like Google, friends, state bodies, or rescue forces. This is in line with other research showing that some people see no benefit in data sharing [5]. They may rarely use applications or stop using them completely if transparency and control over shared data is not ensured [26]. In another study, it was similarly argued by users that possible benefits to society would

Table 5: Which service is switched on? Self-reported status vs. actual status – street interviews

Wi-Fi				Location Services (GPS)				Bluetooth			
Self-reported status		*Actual status*		Self-reported status		*Actual status*		Self-reported status		*Actual status*	
Switched on	Switched off	Switched on	Switched off	Switched on	Switched off	Switched on	Switched off	Switched on	Switched off	Switched on	Switched off
72%	28%	69%	31%	39%	61%	43%	57%	26%	74%	43%	57%
Discrepancy between self-reported activation status and actual status (self-report - actual)											
3%	-3%	/	/	-4%	4%	/	/	-17%	17%	/	/

Table 6: Reasons for switching location services (GPS), Wi-Fi, and Bluetooth off – street interviews.

Why do you activate or deactivate location services (GPS), Wi-Fi, or Bluetooth?		
Category	Examples	Quantity named (N = 58)
Usage need	"I need GPS to use Google Maps"	32
No need to use	"I do not need these services"	14
Privacy reasons	"I do not want to disclose my location"	16
Economic reasons	"Without this service switched on the battery consumption is lower"	9
Other reasons	"Depends on how I feel"	11

have to be overwhelmingly big before a not consented access to personal medical data should be allowed [50]. Generally, the fact that data sharing is linked to the data type and data receiver, is in line with Helen Nissbaum's [38] theory of contextual integrity. This theory states that multiple factors determine personal information flow, among which are attributes (i.e. data types), actors (i.e. data receiver), and transmission principles. Thus, data sharing attitudes and behavior generally are highly volatile and difficult to generalize across data types and involved actors.

Our findings are thus consistent with both the concept of contextual integrity as well as empirical studies that found, for example, that users care about who receives information and the level of detail provided [2, 15].

5.4 Activation of Data Sharing Functionalities

Another question is: Do users also protect themselves from involuntary data sharing by switching off functionalities that allow tracking and data sharing and can even be gateways for crime? In this paper we looked at user activation of Wi-Fi, GPS, Bluetooth as potential data sharing functionalities. We found that more than a quarter of users has GPS and Wi-Fi always activated, with respect to Bluetooth, this applies to 18%. With the German contact tracing Corona-Warn-App depending on switched on Bluetooth and GPS, the rates for permanent activation might currently be higher compared to times before the pandemic. In our interview study we found similar numbers of users having the three functionalities activated at all times. For Bluetooth, 17% of users thought their Bluetooth was switched off but it was in fact activated. Therefore, the self-reports with regard to Bluetooth in our online survey might also underestimate actual settings. This also hints to the conclusion that users are not always aware about which functionalities are activated on their smartphone. Future research should take a look at why people are not aware and how they can be made aware. For example, in the IoT context promising tools to archive this are Personalized Privacy Assistants (PPAs), which can grant the user some kind of control but also need to not overwhelm the users [14]. Similar to secure e-mail and messenger adoption [1, 51] this might also be due to bad usability and missing utility of switching Wi-Fi, GPS, and Bluetooth off, as the most named reason for activating Bluetooth, GPS, and Wi-Fi in both studies was "I need to use it". This again points out the importance of utility and usability in the use of technologies: People turn on the functionalities that they frequently need in order to use tools such as route planning or listening to music via headphones. In our online study the most frequently named reason for switching services off was "economic" reasons, meaning high battery or energy consumption. Privacy and security reasons were named less often, which is in line with other studies stressing the need for more privacy awareness and implementation of privacy recommendations [49]. Consequently, for users to be able to make informed decisions about the data they want to share, they need to be better educated about how to turn Bluetooth, GPS, and Wi-Fi off and importantly about potential risks that may arise from sensor data that is permanently transmitted. Other studies (e.g. [46]) have also shown that users often feel that they generally have little control over their data and that interfaces for their privacy settings are just too complicated. This represents another area in which action and support for users is needed, so that users can handle data sharing responsibly.

6 CONCLUSION

With rising numbers of smartphone users and an increasing numbers of apps with numerous possibilities offering benefits and incentives for sharing private smartphone data, we took users' awareness and willingness to share private smartphone data under investigation. We found most users to view all proposed data types as private, with more women rating data types as private than men. We also found the willingness to share data to differ for diverse data receivers and for sharing conditions. Except for rescue forces, the most frequently named sharing condition for all other entities was on premise (with explicit allowance for the particular situation). Regarding rescue forces the most named sharing condition was "when I am endangered". For Wi-Fi, most users indicated that it is always activated on their phone, compared to most users indicating to activate GPS and Bluetooth only when needed. We did only find small discrepancies (4%) for the self-reported activation status of Wi-Fi and GPS, but a 17% discrepancy concerning Bluetooth. Users seem to be less aware of their Bluetooth status than that of Wi-Fi and GPS. In any case, users need to be made aware of how to activate and deactivate these functionalities on their smartphone, the

potential benefits and risks arising from them, as well as how to secure their private data.

ACKNOWLEDGMENTS

This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and by the Deutsche Forschungsgemeinschaft (DFG) – SFB 1119 (CROSSING) – 236615297 as well as GRK 2050 (Privacy & Trust) – 251805230.

REFERENCES

[1] Ruba Abu-Salma, M. Sasse, Joseph Bonneau, A. Danilova, Alena Naiakshina, and M. Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 137–153. https://doi.org/10.1109/SP.2017.65

[2] Larissa Aldehoff, Meri Dankenbring, and Christian Reuter. 2019. Renouncing Privacy in Crisis Management? People's View on Social Media Monitoring and Surveillance. In *Proceedings of the Information Systems for Crisis Response and Management (ISCRAM)*. ISCRAM Association, València, Spain, 1184–1197.

[3] N. Ali, Md. Lizur Rahman, and I. Jahan. 2019. Security and Privacy Awareness: A Survey for Smartphone User. *International Journal of Advanced Computer Science and Applications* 10 (2019), 483–488.

[4] Yutaka Arakawa and Yuki Matsuda. 2016. Gamification Mechanism for Enhancing a Participatory Urban Sensing: Survey and Practical Results. *Journal of Information Processing* 24 (01 2016), 31–38. https://doi.org/10.2197/ipsjjip.24.31

[5] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 12, 11 pages. https://doi.org/10.1145/2501604.2501616

[6] Kim Bartel Sheehan. 1999. An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing* 13, 4 (1999), 24–38. https://doi.org/10.1002/(SICI)1520-6653(199923)13:4<24::AID-DIR3>3.0.CO;2-O

[7] Susanne Barth and Menno D.T. de Jong. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics* 34, 7 (2017), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

[8] Miriam Bartsch and T. Dienlin. 2016. Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior* 56 (2016), 147–154.

[9] Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. 2004. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society* 20, 5 (2004), 313–324. https://doi.org/10.1080/01972240490507956 arXiv:https://doi.org/10.1080/01972240490507956

[10] Tom Biselli and Christian Reuter. 2021. On the Relationship between IT Privacy and Security Behavior: A Survey among German Private Users. In *Proceedings of the International Conference on Wirtschaftsinformatik (WI)*. AIS, Potsdam, Germany, 1–17. http://www.peasec.de/paper/2021/2021_BiselliReuter_RelationshipITPrivacyandSecurityBehavior_WI.pdf

[11] A.J. Bernheim Brush, John Krumm, and James Scott. 2010. Exploring End User Preferences for Location Obfuscation, Location-Based Services, and the Value of Location. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing* (Copenhagen, Denmark) *(UbiComp '10)*. Association for Computing Machinery, New York, NY, USA, 95—-104. https://doi.org/10.1145/1864349.1864381

[12] Q. H. Cao, I. Khan, R. Farahbakhsh, G. Madhusudan, G. M. Lee, and N. Crespi. 2016. A trust model for data sharing in smart cities. In *2016 IEEE International Conference on Communications (ICC)*. IEEE, Kuala Lumpur, Malaysia, 1–7. https://doi.org/10.1109/ICC.2016.7510834

[13] Hyunghoon Cho, Daphne Ippolito, and Yun William Yu. 2020. Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. arXiv:2003.11511

[14] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1—-13. https://doi.org/10.1145/3313831.3376389

[15] Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location disclosure to social relations: Why, when, & what people want to share. In *CHI 2005: Technology, Safety, Community: Conference Proceedings - Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 81–90.

[16] Adrienne Porter Felt, Serge Egelman, and David Wagner. 2012. I've Got 99 Problems, but Vibration Ain't One: A Survey of Smartphone Users' Concerns. In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices* (Raleigh, North Carolina, USA) *(SPSM '12)*. Association for Computing Machinery, New York, NY, USA, 33—-44. https://doi.org/10.1145/2381934.2381943

[17] Bundesamt für Sicherheit in der Informationstechnik – BSI. 2019. *Sicher unterwegs mit Smartphone, Tablet & Co - Basisschutz leicht gemacht, Tipps zum Umgang mit mobilen Endgeräten*. Technical Report. Bundesamt für Sicherheit in der Informationstechnik – BSI, Bonn, Germany.

[18] Statistisches Bundesamt; Wissenschaftszentrum Berlin für Sozialforschung; Bundesinstitut für Bevölkerungsforschung. 2016. *Datenreport 2016. Ein Sozialbericht für die Bundesrepublik Deutschland*. Technical Report. Statistisches Bundesamt; Wissenschaftszentrum Berlin für Sozialforschung; Bundesinstitut für Bevölkerungsforschung, Bonn, Germany.

[19] H. Gao, C. H. Liu, W. Wang, J. Zhao, Z. Song, X. Su, J. Crowcroft, and K. K. Leung. 2015. A Survey of Incentive Mechanisms for Participatory Sensing. *IEEE Communications Surveys Tutorials* 17, 2 (2015), 918–943. https://doi.org/10.1109/COMST.2014.2387836

[20] Muhammad Habib ur Rehman, Chee Sun Liew, Teh Wah, Junaid Shuja, and Babak Daghighi. 2015. Mining Personal Data Using Smartphones and Wearable Devices: A Survey. *Sensors* 15 (02 2015), 4430–4469. https://doi.org/10.3390/s150204430

[21] Il-Horn Hann, K. Hui, S. Lee, and I. Png. 2002. Online Information Privacy: Measuring the Cost-Benefit Trade-Off. In *ICIS 2002 Proceedings*. ICIS, Barcelona, Spain, 1.

[22] Gabriella M. Harari, N. Lane, R. Wang, Benjamin S Crosier, A. Campbell, and S. Gosling. 2016. Using Smartphones to Collect Behavioral Data in Psychological Science. *Perspectives on Psychological Science* 11 (2016), 838 –854.

[23] Andreas Kamilaris and Andreas Pitsillides. 2016. Mobile Phone Computing and the Internet of Things: A Survey. *IEEE Internet of Things Journal* 3 (12 2016), 1–1. https://doi.org/10.1109/JIOT.2016.2600569

[24] Salil S. Kanhere. 2011. Participatory Sensing: Crowdsourcing Data from Mobile Smartphones in Urban Spaces. In *2011 IEEE 12th International Conference on Mobile Data Management*, Vol. 2. IEEE, Lulea, Sweden, 3–6. https://doi.org/10.1109/mdm.2011.16

[25] Jalaluddin Khan, Haider Abbas, and Jalal Al-Muhtadi. 2015. Survey on Mobile User's Data Privacy Threats and Defense Mechanisms. *Procedia Computer Science* 56 (12 2015), 376–383. https://doi.org/10.1016/j.procs.2015.07.223

[26] M. V. Kleek, I. Liccardi, Reuben Binns, J. Zhao, D. Weitzner, and N. Shadbolt. 2017. Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 5208—-5220.

[27] Hanna Krasnova and Natasha F. Veltri. 2010. Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. In *2010 43rd Hawaii International Conference on System Sciences*. IEEE, Honolulu, HI, USA, 1–10.

[28] Michael Kroker. 2020. *Die Smartphone-Trends 2020: Zahl der Nutzer wächst um 300 Millionen auf 3,5 Milliarden*. WirtschaftsWoche. Retrieved June, 2020 from https://blog.wiwo.de/look-at-it/2020/05/13/die-smartphone-trends-2020-zahl-der-nutzer-waechst-um-300-millionen-auf-35-milliarden/

[29] S. L. Lau and S. M. Sabri Ismail. 2015. Towards a Real-Time Public Transport Data Framework Using Crowd-Sourced Passenger Contributed Data. In *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*. IEEE, Boston, MA, USA, 1–6. https://doi.org/10.1109/VTCFall.2015.7391180

[30] Yao Li, Alfred Kobsa, Bart P. Knijnenburg, and M-H. Carolyn Nguyen. 2017. Cross-Cultural Privacy Prediction. In *Proceedings on Privacy Enhancing Technologies*. De Gruyter Open, 113–132. https://doi.org/10.1515/popets-2017-0019

[31] Christian Masdeval and Adriano Veloso. 2015. Mining citizen emotions to estimate the urgency of urban issues. *Information Systems* 54 (06 2015). https://doi.org/10.1016/j.is.2015.06.008

[32] Philipp Mayring. 2014. *Qualitative content analysis - theoretical foundation, basic procedures and software solution*. Klagenfurt, Austria.

[33] Helfried Moosbrugger and Augustin Kelava. 2012. *Testtheorie und Fragebogenkonstruktion 2. Auflage*. Springer-Verlag Berlin Heidelberg New York, Berlin, Heidelberg, Germany.

[34] Deborah M. Moscardelli and Richard L. Divine. 2007. Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy-Protecting Behaviors. *Family and Consumer Sciences Research Journal* 35 (2007), 232–252.

[35] Yuri Nakagawa, Yuuki Matsuda, and Tetsuro Ogi. 2015. Framework for handling personal data: analysis of buying information by questionnaire. *International Journal of Big Data Intelligence* 2 (01 2015), 223. https://doi.org/10.1504/IJBDI.2015.072159

[36] J. Nicholas, Katie Shilton, S. Schueller, Elizabeth L Gray, M. Kwasny, and D. Mohr. 2019. The Role of Data Type and Recipient in Individuals' Perspectives on

Sharing Passively Collected Smartphone Data for Mental Health: Cross-Sectional Questionnaire Study. *JMIR mHealth and uHealth* 7, 4 (2019), e12578.

[37] Evangelos Niforatos, Athanasios Vourvopoulos, and Marc Langheinrich. 2016. Understanding the Potential of Human-Machine Crowdsourcing for Weather Data. *International Journal of Human-Computer Studies* 102 (10 2016). https://doi.org/10.1016/j.ijhcs.2016.10.002

[38] Helen Nissenbaum. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press, Stanford, USA.

[39] Y. Park, Scott W. Campbell, and Nojin Kwak. 2012. Affect, cognition and reward: Predictors of privacy protection online. *Comput. Hum. Behav.* 28 (2012), 1019–1027.

[40] Yong Jin Park and Mo Jones Jang. 2014. Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior* 38 (09 2014), 296—-303. https://doi.org/10.1016/j.chb.2014.05.041

[41] Sofia Ranchordas. 2019. Nudging citizens through technology in smart cities. *International Review of Law, Computers & Technology* 34 (03 2019), 1–23. https://doi.org/10.1080/13600869.2019.1590928

[42] Christian Reuter, Marc-André Kaufhold, Stefka Schmid, Thomas Spielhofer, and Anna Hahne. 2019. The impact of risk cultures: Citizens' perception of social media use in emergencies across Europe. *Technological Forecasting and Social Change* 148 (11 2019), 119724. https://doi.org/10.1016/j.techfore.2019.119724

[43] Robert-Koch-Institut. 2021. *Übersicht zu aktuellen und früherer Zahlen und Fakten zur Corona-Warn-App.* RKI. https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/WarnApp_KennzahlenTab.html

[44] Sandro Rodriguez Garzon and Bersant Deva. 2019. Sensafety: Crowdsourcing the Urban Sense of Safety. *Advances in cartography and GIScience of the ICA* 2, 12 (2019). https://doi.org/10.5194/ica-adv-2-12-2019

[45] Mark Rowan and Josh Dehlinger. 2014. Observed Gender Differences in Privacy Concerns and Behaviors of Mobile Device End Users. *Procedia Computer Science* 37 (2014), 340–347. https://doi.org/10.1016/j.procs.2014.08.050 The 5th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2014)/ The 4th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2014)/ Affiliated Workshops.

[46] Manuel Rudolph and Svenja Polst. 2018. Satisfying and Efficient Privacy Settings. In *Mensch und Computer 2018 - Tagungsband*, Raimund Dachselt and Gerhard Weber (Eds.). Gesellschaft für Informatik e.V., Bonn, 215–224. https://doi.org/10.18420/muc2018-mci-0192

[47] Christine Utz, Steffen Becker, Theodor Schnitzler, Florian M. Farke, Franziska Herbert, Leonie Schaewitz, Martin Degeling, and Markus Dürmuth. 2021. Apps Against the Spread: Privacy Implications and User Acceptance of COVID-19-Related Smartphone Apps on Three Continents. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 70, 22 pages. https://doi.org/10.1145/3411764.3445517

[48] Johann Vincent, Christine Porquet, Maroua Borsali, and Harold Leboulanger. 2011. Privacy Protection for Smartphones: An Ontology-Based Firewall. In *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication*, Claudio A. Ardagna and Jianying Zhou (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 371–380.

[49] Bryan Watson and Jun Zheng. 2017. On the User Awareness of Mobile Security Recommendations. In *Proceedings of the SouthEast Conference* (Kennesaw, GA, USA) *(ACM SE '17)*. Association for Computing Machinery, New York, NY, USA, 120—-127. https://doi.org/10.1145/3077286.3077563

[50] Colin Watson and Jan David Smeddinck. 2020. Unconsented Data Transfusions: Attitudes towards Extracting Personal Device Data for Public Health Emergencies. In *Proceedings of the Conference on Mensch Und Computer* (Magdeburg, Germany) *(MuC '20)*. Association for Computing Machinery, New York, NY, USA, 205—-209. https://doi.org/10.1145/3404983.3409994

[51] A. Whitten and J. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium*. USENIX Association, Washington, D.C., 169—-184. https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50

A APPENDICES

A.1 Online Survey Questions

Table 7: Online Survey Questions. Used abbreviations: MC = Multiple Choice

ID	Question	Original Question (German)
QO01	Do you own a smartphone? (Yes / No / Don't know)	Besitzen Sie ein Smartphone? (Ja / Nein / Weiß nicht)
QO02	When is your smartphone turned on? (Always / When I leave home / At daytime / Only when using it)	Wann ist Ihr Smartphone eingeschaltet? (Immer, außer der Akku ist leer / Nur wenn ich das Haus verlasse / Nur tagsüber / Nur für die konkrete Dauer, in der ich etwas mit dem Smartphone tue)
QO03	Which operating system does your smartphone have? (Android / iOS / Other / Don't know)	Welches Betriebssystem hat Ihr Smartphone? (Android / iOs / Sonstiges / Weiß ich nicht)
QO04	Why are you using this operating system? (MC: Preinstalled / Security reasons / Known / Other)	Wieso haben Sie dieses Betriebssystem auf Ihrem Smartphone? (MC: Weil es bei meinem Handy bereits installiert war / Weil ich mir dadurch mehr Sicherheit verspreche / Weil ich mich mit diesem Betriebssystem auskenne / Sonstiges: Freitext)
QO05	What is activated at which times? (Axis1: WIFI, Location services (e.g., GPS), Bluetooth; Axis 2: Always / Never / When using it / At daytime / Don't care / Don't know)	Bei meinem Smartphone sind (Achse 1: W-Lan, Standortdienste (bspw. GPS), Bluetooth / Achse 2: Immer aktiviert / Immer deaktiviert / Nur aktiviert, wenn ich es brauche / Nachts deaktiviert, tags aktiviert / Darauf achte ich nicht / Ich weiß nicht, was das ist)
QO06	When and why do you activate or deactivate location services, WIFI, or Bluetooth? (text)	Wieso und wozu aktivieren/deaktivieren Sie Standortdienste, WLAN oder Bluetooth? (Freitext)
QO07	Why don't you own a smartphone? (text, when Q1 "no")	Wieso besitzen Sie kein Smartphone? (Freitext)
QO08	Do you own smart wearables? (yes / no / don't know)	Besitzen Sie Smart Wearables? (Ja / Nein / Weiß nicht)
QO09	Which smart wearables do you use and for which purpose? (text)	Welche Smart Wearables nutzen Sie und wofür? (Freitext)
QO10	Why don't you own or use smart wearables? (text)	Wieso besitzen und/oder benutzen Sie keine Smart Wearables? (Freitext)
QO11	… are perceived as private data from me (name / address / birthday / account data / identity card number / my files (photos, documents, etc.) / my location data / my communication data (messenger, phone, etc.), other: text)	Private Daten sind für mich (MC: Mein Name / Meine Adresse / Mein Geburtsdatum / Meine Kontodaten / Meine Personalausweisnummer / Meine Dateien (Fotos, Dokumente, etc.) / Meine Bewegungsdaten (Wann war ich wo? - GPS-Daten) / Meine Kommunikationsdaten (Inhalte von Messenger-Nachrichten, Telefonate, etc.) / Sonstiges: Freitext)
QO12	Who shall be able to see my private data in which cases? (Axis 1: persons I chose, services I chose (e.g. Google), state actors as government, municipal office, etc., state actors as military, secret services, police etc., rescue teams and emergency personnel; Axis 2: Never / Always / With single permissions / If I'm in danger / If potential danger for humans can be reduced / If human lives can be saved through using my data	Wer darf wann meine für mich privaten Daten einsehen? (Achse 1: Von mir bestimmte Personen / Von mir bestimmte Dienste, wie Google, Anwendungen, etc. / Kreuzen Sie die zweite Spalte von links an / staatliche Akteure wie Regierung, Bürgeramt, etc. / staatliche Akteure wie Militär, Geheimdienste, Polizei, etc. / Rettungskräfte, wie Feuerwehr, Hilfs- und Rettungsorganisationen, etc.) (Achse 2: Können meine privaten Daten nie einsehen / Können meine Privaten Daten Immer einsehen / Können meine Daten einsehen, wenn ich es ihnen jeweils in einer Situation explizit erlaube /Können meine Daten einsehen, wenn ich in Gefahr bin / Können meine Daten einsehen, wenn die Gefährdung von Menschenleben dadurch potenziell verhindert werden kann / Können meine Daten einsehen, wenn Menschenleben dadurch gerettet werden können)
QO13	I think I would be more willing to share my personal data to help persons I know personally (Yes / Rather yes / This makes no difference / Rather no / No / Don't know)	Ich wäre vermutlich eher bereit meine Daten automatisch mit staatlichen Akteuren oder Rettungskräften zu teilen, wenn ich die Person, die in einer Notsituation ist, persönlich kenne. (Ja / Eher ja / Macht keinen Unterschied / Eher nein / Nein / Keine Ahnung)

A.2 Street Interview Questions

Table 8: Street Interview Questions

ID	Question	Original Questions (German)
D1	Gender	Geschlecht
D2	Education Level	Schulabschluss
D3	Age	Alter
QS1	Do you own a smartphone? (Yes / No / Don't know / Other)	Besitzen Sie ein Smartphone? (Ja / Nein / Weiß nicht / Keine Angabe)
QS2	When is your smartphone switched on? (Always / Only when I leave my house / Only in the daytime / Only for the exact amount of time I actively use my smartphone / Other:)	Wann ist Ihr Smartphone eingeschaltet? (Immer (außer der Akku ist leer) / Nur wenn ich das Haus verlasse / Nur tagsüber / Nur für die konkrete Dauer, in der ich etwas mit dem Smartphone tue / Anderes: Freitext)
QS3	Which operating system does your smartphone have? (Android / iOS / Other: text)	Welches Betriebssystem hat Ihr Smartphone? (Android / iOs / Sonstiges: Freitext)
QS4	Why is this operating system installed on your smartphone? (Preinstalled / Security / Experience / Other: text)	Wieso haben Sie dieses Betriebssystem auf Ihrem Smartphone? (Weil es bei meinem Handy bereits installiert war / Weil ich mir dadurch mehr Sicherheit verspreche / Weil ich mich mit diesem Betriebssystem auskenne / Sonstiges: Freitext)
QS5	On my smartphone … are … active (Axis 1: WIFI, GPS, Bluetooth; Axis2: Always / Never / When actively used / Only during daytime / Don't care / Don't know). Why?	Bei meinem Smartphone sind (Achse 1: W-LAN, Standortdienste (bspw. GPS), Bluetooth / Achse 2: Immer aktiviert / Immer deaktiviert / Nur aktiviert, wenn ich es brauche / Nachts deaktiviert, tags aktiviert / Darauf achte ich nicht / Ich weiß nicht, was das ist)
QS6	Smart Wearables are e.g. fitness trackers or smart watches. Do you own such smart wearables? If yes, which? If no, why not?	Smart Wearables sind bspw. Fitnesstracker oder Smart Watches. Besitzen Sie Smart Wearables? Wenn ja, welche? Wieso? Wieso nicht?
QS7	Do you think that WIFI, GPS, and Bluetooth are activated on your smartphone right now? (Axis1: WIFI, GPS, Bluetooth; Axis2: Yes / No)	Glauben Sie, dass auf Ihrem Smartphone gerade W-LAN, GPS oder Bluetooth aktiviert sind? (Achse 1: W-LAN / GPS / Bluetooth) (Achse 2: Ja / Nein)
QS8	Let's have a look which functions are active! (Axis1: WIFI, GPS, Bluetooth; Axis2: Yes / No)	Lassen Sie uns nachsehen was gerade aktiv ist! (Achse 1: W-LAN / GPS / Bluetooth) (Achse 2: Ja / Nein)